

(12) UK Patent Application (19) GB (11) 2 154 344 A

(43) Application published 4 Sep 1985

(21) Application No 8503481

(22) Date of filing 11 Feb 1985

(30) Priority data

(31) 8403699
8416241

(32) 13 Feb 1984
26 Jun 1984

(33) GB

(51) INT CL⁴
G06F 12/14

(52) Domestic classification
G4A AP

(56) Documents cited
GB A 2121569 EP A2 0131421

(58) Field of search
G4A
H4P

(71) Applicant
National Research Development Corporation (United Kingdom),
101 Newington Causeway, London SE1 6BU

(72) Inventor
Donald Watts Davies

(74) Agent and/or Address for Service
C Hasler,
National Research Development Corporation, 101
Newington Causeway, London SE1 6BU

(54) Apparatus and methods for granting access to computers

(57) When a computer user is granted access to certain capabilities of a computer he is often given a password signifying these capabilities. A problem arises in that unauthorised users may copy the password and so gain access to the capabilities. In the present invention an enciphered message relating to capabilities is stored in the tamper-resistant store 14 of a token 10. The store 14 also holds the secret key of a public key encryption system so that the enciphered message and a distinctive message can be transformed ("signed") using the secret key and passed to the computer. The corresponding public key may then be used by the computer to carry out an inverse transverse form and check the enciphered and distinctive messages against signals sent from the token. If this check is successful the required access is granted. Preferably the public key is part of the enciphered message, especially where the token grants access to a distributed or fragmented computer system, since this avoids the necessity of making public keys available throughout a computer system.

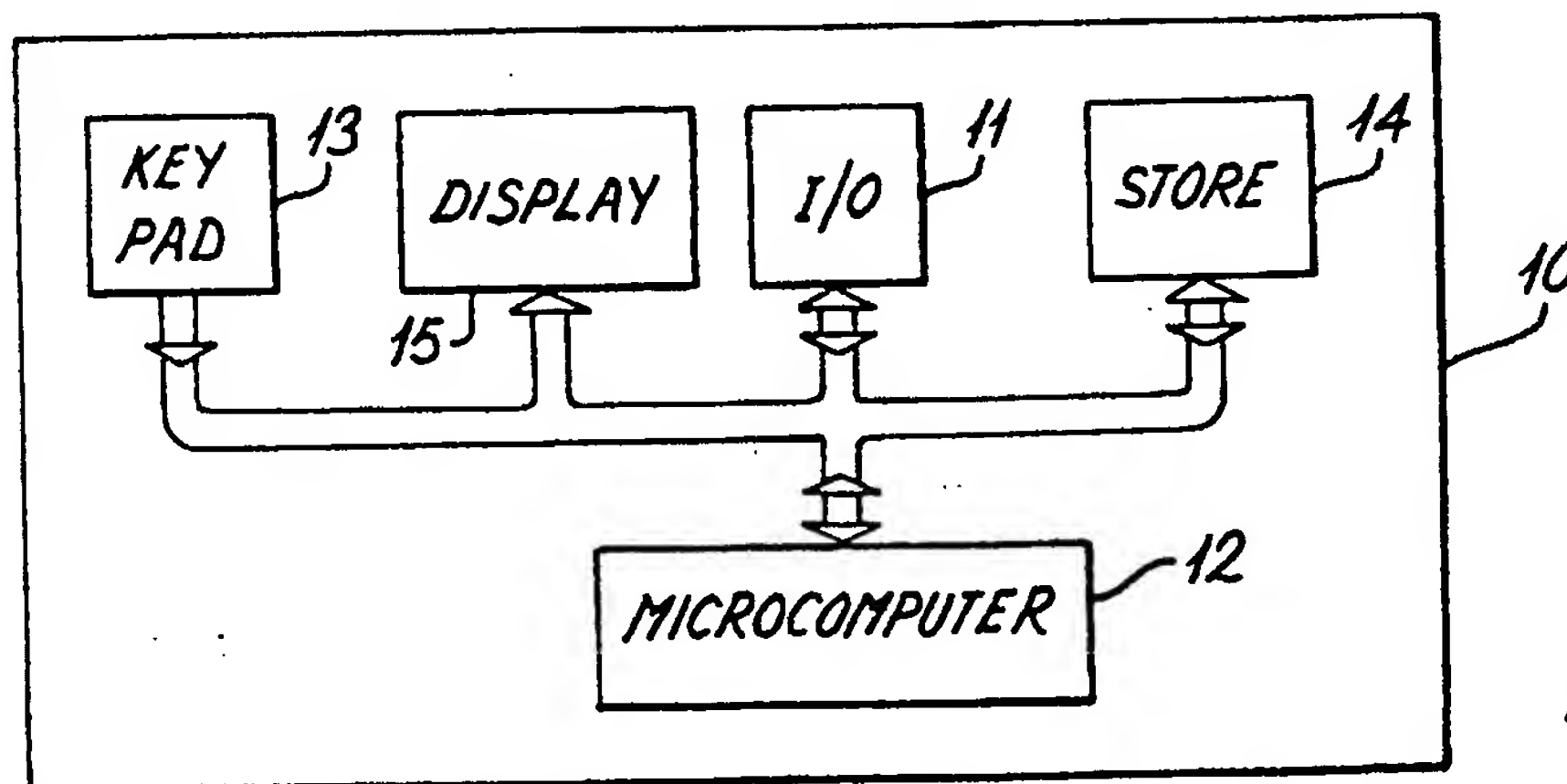


Fig. 1

GB 2 154 344 A

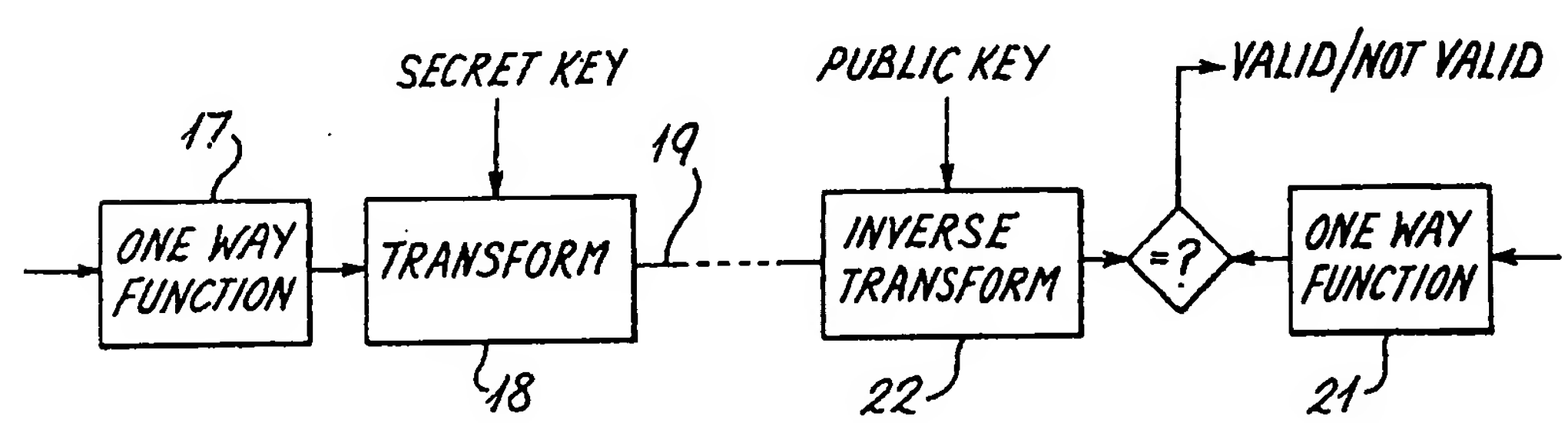
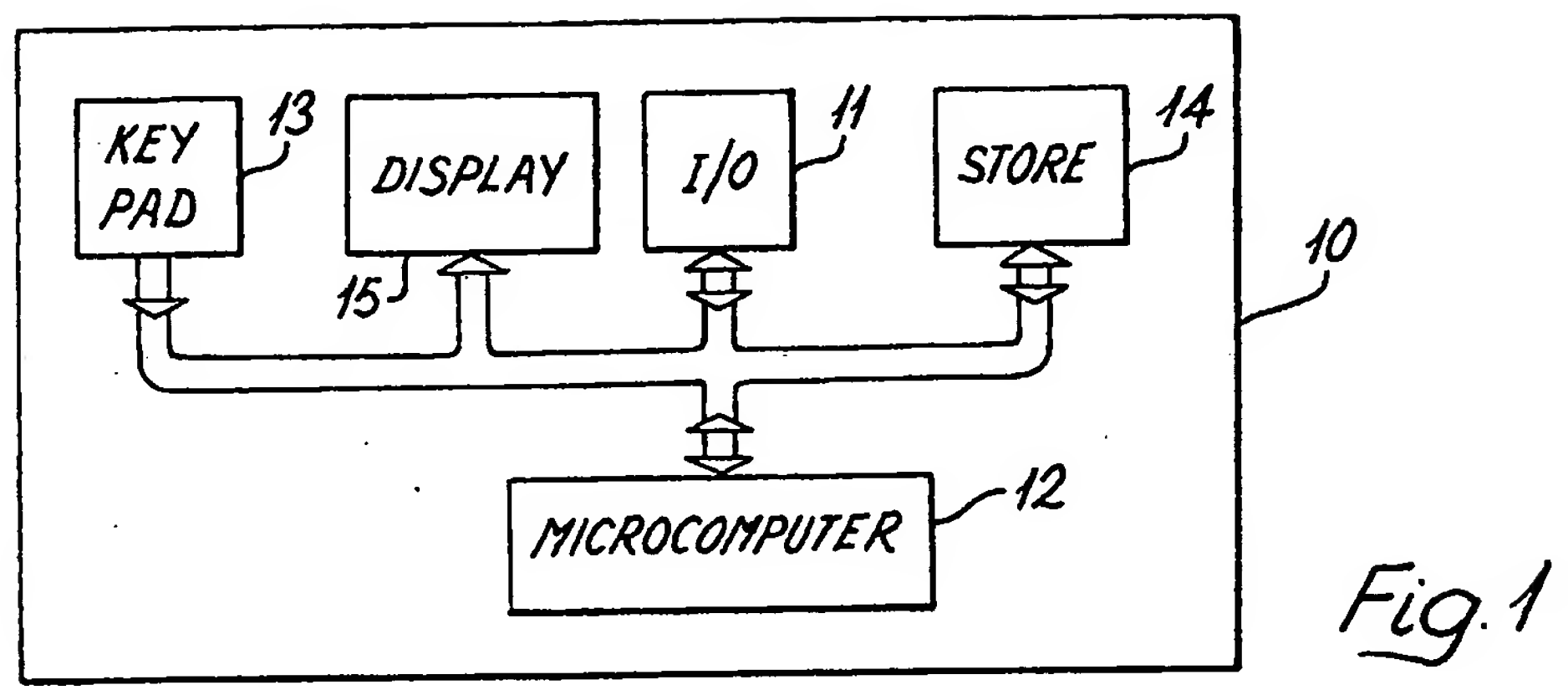


Fig. 2

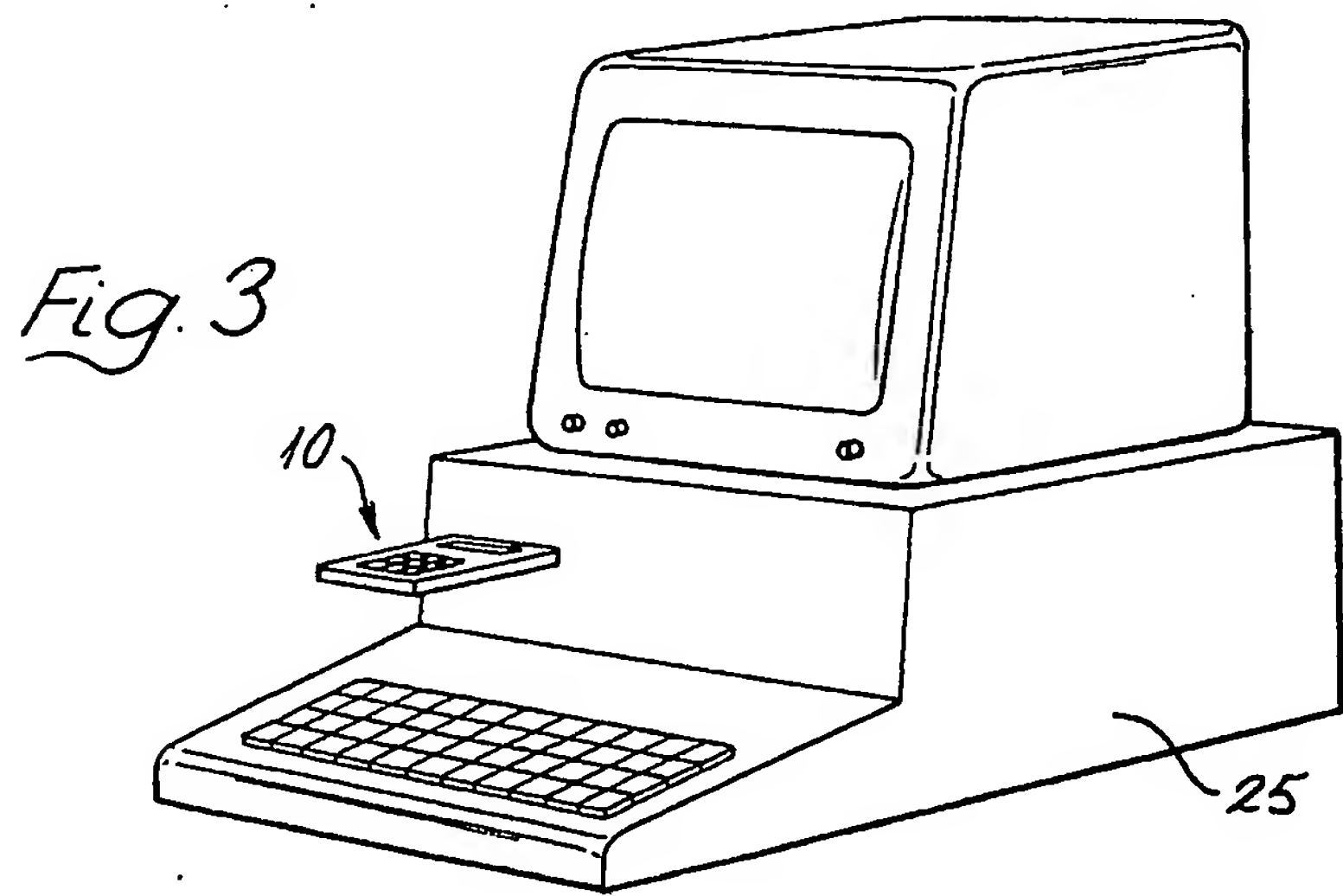


Fig. 3

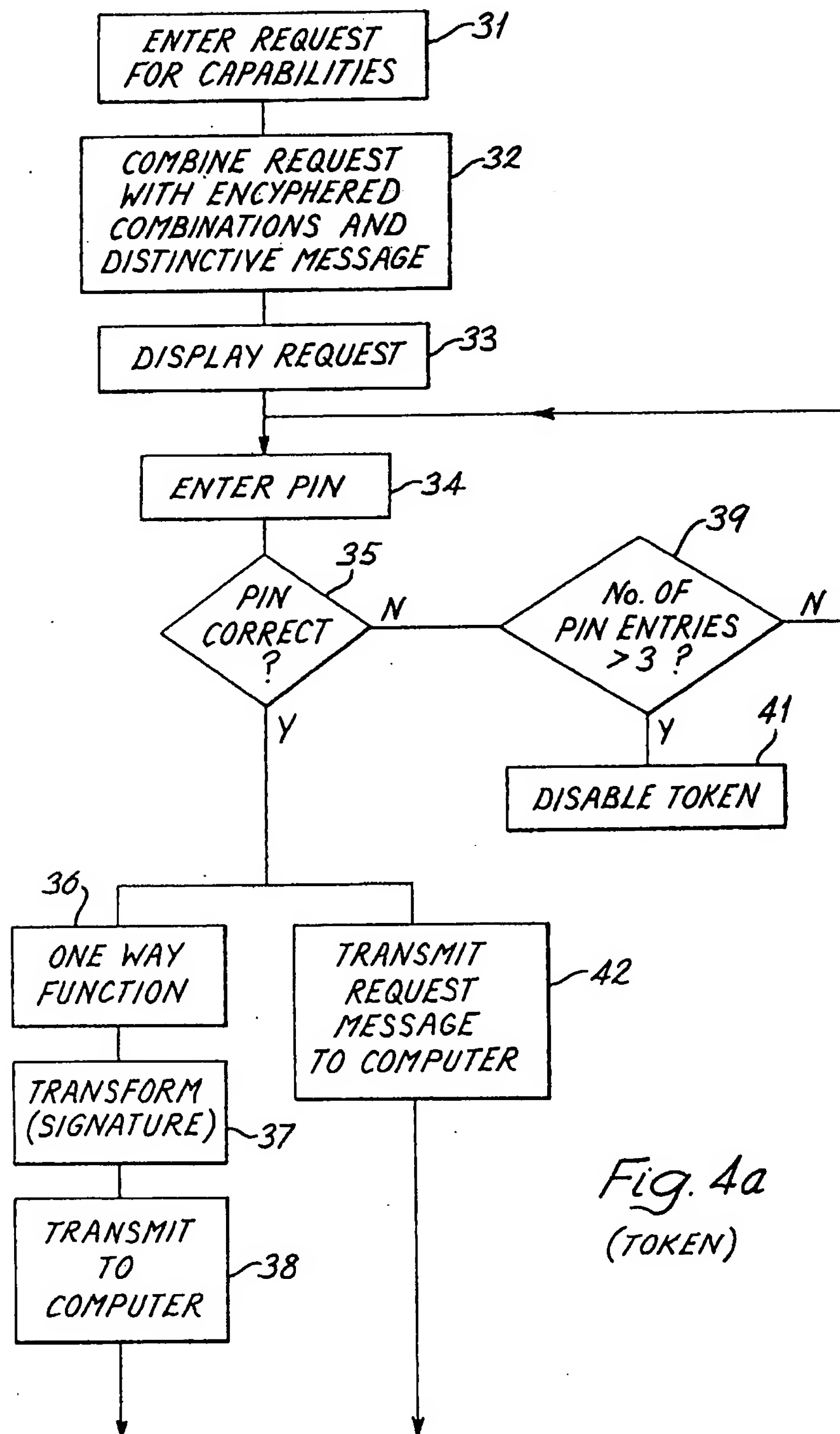


Fig. 4a
(TOKEN)

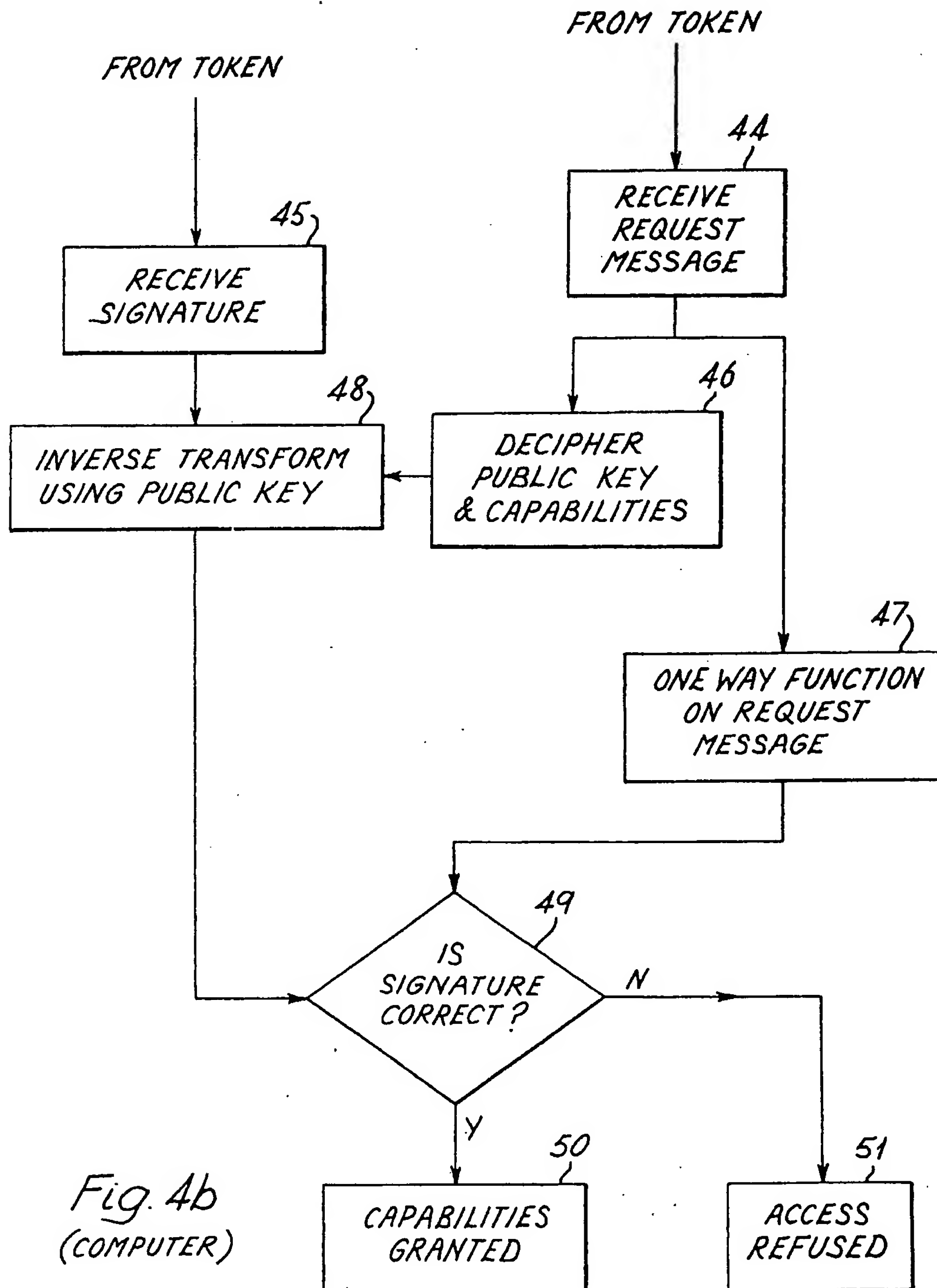


Fig. 4b
(COMPUTER)

SPECIFICATION

Apparatus and methods for granting access to computers

- 5 The present invention relates to methods and apparatus for providing authorised users with access to restricted facilities such as "capabilities" of a computer. Any access facility offered by a computer can be coded in a record known as a capability and associated with a user who is to be allowed use of that facility. The coded record may relate to a certain mode of access to stored file, for example read, write, append, run program, and the record then contains at least
- 10 two fields:
file identity, access mode.
- For each user, a file or files of capabilities are stored in the computer. As part of the rules of access control, these are carefully protected by hardware or software methods to prevent illegal manipulation of capabilities, such as illegally creating new ones or copying those belonging to
- 15 other users. Therefore, capabilities are not allowed outside the computer's protected store and are treated in a different way from other stored data.
- The term "computer" in this specification comprises a distributed system of separate machines as well as a single machine.
- If a user is given information, for example in the form of a password and the numbers of
- 20 certain files, so that he can access the computer, he can also pass this information on to another user. This is so even if the first mentioned user is only allowed an enciphered form of the file numbers which the computer translates before giving access, and may do so in a way which gives only limited specified capabilities to the user. Further, owners of data or programs may wish to give an access message to certain other persons, such as licensees, but not wish to have
- 25 this message copied.
- Authentication for other purposes than providing access to computer capabilities has been achieved using a public key encryption system in which, for example, a message can be transformed using a secret key and transformed back to its original form (inverse transformed) using a public key but the secret key cannot be determined from a knowledge of the public key
- 30 or from transformed messages. Public key encryption systems are well known and have been described many times, notably by Rivest, Shamir and Adleman in "A method for obtaining digital signatures and public key cryptosystems", Communication of the Association for Computing Machinery, Volume 21, No. 2, February 1978, page 120. Digital signatures of another kind have been described by Ong, Schnorr and Shamir.
- 35 In order to authenticate a message the signer has in some known methods employed a computer to calculate a digest of the message, for example using a one-way function, and then he has entered his secret key to transform the result. The transformed digest together with the message itself are passed to the recipient who uses the public key to inverse transform the transformed digest and he compares the result with the digest which he calculates himself
- 40 according to known rules. If the two are equal then the message is authenticated. This procedure is described by D.W. Davies and W.L Price in the paper "The application of digital signatures based on public key cryptosystems", Proc. 5th ICCS, Atlanta Ga., October 1980.
- In this specification "transformation" or "transforming" are operations carried out in a system which has two keys either of which may be used for transformation when the other key is
- 45 required for inverse transformation. However the knowledge of one key does not allow the other key to be determined even when a transformed message is available, thus preventing both of the operations of transformation and inverse transformation.
- Authentication apparatus is known for the purpose of automatically creating digital messages using input messages from a particular source. The automatically created messages can be
- 50 positively identified as originating from the source if the input messages are available. Such automatically created messages are known as digital signatures and such apparatus is herein-after referred to as a signature token.
- To overcome the above-mentioned problem of giving access to computer capabilities an authentication method, apparatus and a programmed computer according to first, second and
- 55 third aspects of the invention are provided.
- An authentication method according to the first aspect of the invention for granting access to a computer comprises
- as a preliminary step,
- storing a secret key in authentication apparatus together with enciphered information
- 60 representing the capabilities to be granted by the computer and either the public key corresponding to the secret key or information which identifies the public key,
- and as steps employed when access is to be granted,
- using the authentication apparatus to form one part of an output message to contain the enciphered information and transforming as hereinbefore defined, using the secret key, a
- 65 distinctive message to generate another part of the output message,

using the computer to decipher the enciphered information and inverse transform the said other part of the output message using the public key, and

comparing digital signals representing the result of the inverse transform with digital signals representing the distinctive message or information derived therefrom and granting the required access only if the digital signals compared are the same.

Authentication apparatus according to the second aspect of the invention for providing access to a computer comprises

a store containing a secret key for carrying out a transformation as hereinbefore defined and enciphered information representing capabilities to be granted by a computer and either the public key corresponding to the secret key or information which identifies the public key, input/output means for receiving and transmitting electrical digital messages to, and from, the apparatus, and

means for forming one part of an output message to contain the enciphered information and for transforming, using the secret key, a distinctive message, or a message determined therefrom, to generate another part of the output message.

An advantage of the invention is that capabilities are stored outside the computer or computer system in a secure way so reducing the storage requirements of the computer or system. This advantage is significant where many users have access to many computers, since capabilities are stored only once.

The authentication apparatus of the second aspect of the invention may be regarded as digitally signing the distinctive message and may therefore be regarded as a special form of a signature token.

The distinctive message may comprise at least one of the following: an indication of where the output message stands in a sequence of such messages, the time of day, the date and a random number.

Preferably the apparatus, in operation, combines the distinctive message and the enciphered message before transforming the combination to form the said other part of the output message.

According to the third aspect of the invention there is provided a computer programmed

to decipher one part of a message transmitted to the computer, the said one part containing, in enciphered form, information representing access to computer capabilities and a public key or information identifying the public key, and

to inverse transform another part of the message using the public key to determine whether the result after inverse transformation contains a predetermined distinctive message, and

if so to provide the access conferred.

Where the said other part of the output message from the authentication apparatus is expected to include, in transformed form, the said one part of the output message, the computer is programmed to provide access to capabilities only if on inverse transforming the said other part of the output message, the public key and the capabilities are so contained in the said one part.

The authentication apparatus preferably pre-processes messages in the way mentioned above to provide shorter messages for transformation and the computer carries out the same pre-processing before granting access on the basis of a correct inverse transformed message.

By using a signature token to sign the distinctive message and preferably the enciphered message at the time a request for access is made, the use of copied access messages is prevented.

According to a fourth aspect of the present invention there is provided authentication apparatus which can easily be held in one hand and comprises

input/output means for receiving electrical digital messages to be "transformed" and for transmitting transformed messages,

an electrical store which is physically tamper-resistant holding a secret electrical digital key for use in carrying out transformation as hereinbefore defined, the key being so stored that it cannot be read out by applying signals to the apparatus.

transformation means for transforming, when enabled, an input message or a message related thereto using the secret key to generate an output message for transmission by the input/output means,

enabling means for enabling the transformation means on receipt of a personal input to the apparatus direct from a particular person or at least one of a particular group of persons, the personal input being specific to that person or those persons, and

a display for displaying at least part of the message to be transformed.

The enabling means may include a keyboard and means for recognising a personal identification number (PIN), transformation only taking place when the correct PIN number has been entered by way of the keyboard. An alternative authorising means may include a graphical input means and means for recognising a signature written thereon. Where the enabling means includes a keyboard, the need to send the PIN through a separate terminal which may not be completely secure is avoided.

Certain embodiments of the invention are now described with reference to the accompanying drawings, in which:—

Figure 1 is a block diagram of apparatus according to the invention,

Figure 2 is a flow diagram illustrating the generation of a digital signature,

5 *Figure 3* is a schematic view of apparatus of Fig. 1 coupled to a computer terminal, and

Figures 4a and 4b are flow diagrams of a request for access to a computer system.

An essential part of controlling access to capabilities of computer systems is apparatus, for example a token which can store certain information, as is explained later, and provide a digital signature. Such a token is therefore first described.

10 In Fig. 1 the housing for a token is represented by a line 10 and may for example be a thin plastic card containing integrated circuits, or a small container. Many other suitable housings can be envisaged, the main requirements being small size for convenience of handling and difficulty of removing the, or at least one of the, integrated circuits without damaging it.

The token includes an input/output port 11 which may take many forms such as electrical 15 contacts, or a transmitter and receiver for ultrasonic, induction, optical or electromagnetic linkage. Where the housing is in the form of a card or flat container, it may be placed on a shelf to allow optical or other communication to be established, and a light source may be provided to project light on to solar cells on the token to provide power for the integrated circuits. The token may instead be powered by way of electrical contacts, induction or by a battery.

20 The token includes a microcomputer 12 whose functions include recognising a personal identification number (PIN) entered by way of a key pad 13, using a one-way function to transform data entered by way of the port 11, and transforming the result using the RSA algorithm mentioned above and a secret key held in a store 14. In order to safeguard the secret key the store 14 is tamper-resistant and may comprise a volatile store located in a module which 25 also contains a battery or battery connections for the store, the module being so constructed that the store is cleared if an attempt is made to obtain the secret key by opening the module. The token may include means for overwriting the contents of the store when power is reduced or removed from it or when a short circuit is applied to the power supply of the token. In addition the store may be attached to a pre-stressed member which breaks it should an attempt 30 be made to open the housing or a module containing the store.

The token is so constructed and/or programmed that it is impossible to read out this key by way of the input/output port 11 regardless of what signals are applied to the port.

The microcomputer 12 also controls a display 13 to display the type of operation being carried out, for example access to a computer, and also other information which may be 35 relevant.

When a digital signature is required information to be signed is represented in digital electronic form and handled according to the flow diagram of Fig. 2. The information is passed as digital signals by way of the port 11 to the token where the user enters his PIN via the key pad 13, and the microcomputer 12 checks this number. If satisfactory the microcomputer pre- 40 processes the information in an operation 17 according to a stored program. The pre-processing is carried out using a one-way (that is non-reversible function which is not secret but provides an output which depends on every item making up the information. A suitable method of carrying out pre-processing is described by D.W. Davies and W.L. Price in the above-mentioned paper. The resultant message must be drawn from a large set so that if a fraudulent change were made 45 in the message it would be almost impossible to find a suitable change which on transformation would result in the same resultant message. One reason for carrying out the transformation is that the time taken for transformation is reduced to avoid intolerably long transformation times.

Using the public key encryption system and the secret key held by the token the number derived by means of the one-way function is transformed by the microcomputer again using a 50 stored program in an operation 18 and the number obtained is the digital signature which is transmitted with the plain text. In this way neither the secret key nor the PIN leaves the token 10 and therefore they cannot be copied.

In order to validate the signature generated in the way described above, the message passed to the token, which for computer access applications is locally available, is processed using the 55 same one-way function as is used in operation 17 by carrying out a further operation 21 in a computer (not shown) in Fig. 2. In addition the signature transmitted to the checking computer as indicated by a line 19 is inverse transformed in an operation 22 using the originator's public key. The signature is only validated if operations 21 and 22 both provide the same number.

Although the information and signature can be copied, the information cannot be altered to 60 change any item since if such a change were made a new signature would be required or the authentication procedure would fail. Only the authorised signatory using the correct token can provide a new signature.

An example of controlling access to capabilities of a computer system will now be considered. Certain files are to be accessed only by entering a specific message which identifies the file and 65 whether it can be read, amended or enlarged. The message therefore confers a capability of the

computer to a person who knows the message. If it is required to prevent forgery of these messages, a particular user may be given a message in enciphered form and when the user enters this form the computer system deciphers it to provide access to the required file. However the user who is given the enciphered form can pass it on to other users who may not be authorised for access to this particular file. The problem can be overcome by a method which is now described.

A public key and a corresponding secret key are created and the secret key is sealed in a signature token such as that of Fig. 1. According to the invention capabilities are also stored by a user and any computer which is to generate capabilities for storage by a user must first identify the user. To do this the user's identity is established in some way and the public key of the user's token, pk , is introduced to the computer. For example, the user may become a subscriber to a commercial system, where the user pays for the service received. In another example, the computer's facilities may be restricted or confidential, and then the user's acceptability is attested by another user, such as a responsible officer.

The computer or system granting capabilities employs a secret key kos to encipher capabilities for external storage. The capabilities are usually enciphered together with the user's public key and the enciphered combination can be expressed as:—

$E_{kos}(pk, \text{file identity, access mode})$

These data, or similar data for other capabilities, link the user identity represented by the key pk with the coded form of the capability as used internally. In an alternative and shorter form, the key pk may be replaced by the user identity and a separate table in the computer gives the key pk as a function of user identity. However it is advantageous to use pk as will be described below. Because the key kos is a secret of the computer, new capabilities for external storage cannot be created by users. The cipher used may be a symmetric cipher, with kos as its key, or it can be a public key cipher with secret key kos . The public key cipher is most useful in a fragmented system, as described below.

The enciphered combinations are stored in the token which is then ready for use. Alternatively these combinations and the secret key may be stored in the user's workstation. More than one enciphered combination can be stored giving different capabilities or groups of capabilities and the combinations are then so stored that the function of each can be identified and the required combination selected for use.

The token (or the user's workstation may now be coupled (for example by plugging in) to a terminal (see Fig. 3) of the, or one of the computers of a system and caused to initiate a request for access (operation 31 of Fig. 4a which relates to the token) by making an appropriate entry on its keyboard. A request for access is started by constructing (operation 32) an access request message, for example:

access request, list of enciphered combinations (containing capabilities), sequence number of date/time.

The sequence number of date/time are considered to be one form of a distinctive message, and this message may alternatively be previously obtained from the computer and may be instead of, or in addition to, the sequence number or the time and date comprise a random number. If the distinctive message is obtained previously it is now combined, usually by concatenation, by the token with a signal representing the request and that at least one of the above-mentioned enciphered combinations. The signature token indicates on its display (operation 33) that an access request message is to be signed, the user enters his PIN (operation 34) and if this is correct (test 35), the request message (access request, list of enciphered combinations sequence number or date/time) is sent to the computer in an operation 42, and the one-way function is applied in an operation 36, the signature is calculated using the stored secret key (operation 37) and sent to the computer (operation 38). This process has an additional step to that described in connection with Fig. 2 in that the sequence number, data/time or the distinctive message which can be regarded in relation to Fig. 2 as the input for the operation 18 (if the operation 17 is omitted) is combined with the request and the enciphered combination before the signature is generated.

The signature can be represented as
 $\{ \text{Request, } E_{kos}(Ct, pk), X \}$ signature
 where E_{kos} represents enciphering by the computer using the master key kos ,
 Ct represents the access message or capability conferred on the user,
 pk represents the public key corresponding to the secret key held by the token, and
 X represents the distinctive message.

If the PIN is incorrectly entered more than three times the token is disabled (test 39 and operation 41).

Both the request message and the signature are received in operations 44 and 45 (see Fig. 4b relating to the computer) by the computer from the token. The computer uses the key kos to decipher the public key and the capabilities (operation 46) and then carries out the one-way function (operation 47). If more than one enciphered combination is received the computer may

verify that all the public keys are the same. In an operation 48 the public key is used to inverse transform the signature and then a test 49 is carried out to check the signature by comparing the access message (after the one-way function obtained by way of operations 46 and 47) with the result obtained by way of operations 45 and 46. If the signature is verified, the access message is used to confer the capabilities requested (operation 50), otherwise access is refused (operation 51).

The sequence number or date and time is included in the request in order to prevent the re-use of the message at a later time. If a sequence number is used, the computer is able to check the correct sequence using a record of the last sequence number from this user. Such checking may be relaxed if the sequence number is administered by the token.

If the message which is to be signed is lengthy pre-processing (operation 36) to form a shorter message is used together with the corresponding operation 47 but otherwise these operations may be omitted.

As an alternative to storing the public key in the token, the request may contain the user identity when the computer extracts the public key from its files. Then in operation 46, the public key is identified for use in operation 48 from the identifying information in the request.

In this way the capability given to the signature token holder can only be used when the token is interfaced with a terminal, that is in effect, when he is present. Copying of capabilities for use by another person is thus prevented.

The application of the signature token for access to computer systems described above is particularly useful where a computer system is widely distributed, for example between several countries, since the holder of a token can move from one country to another and use his token at any terminal in the system. The token may contain a number of different capabilities which apply in different areas and give access to local capabilities only.

Most distributed computer systems are connected by communication networks so they can operate as a single system. It is sometimes more convenient in widespread systems to use only off-line connections, sending files by bulk transmissions at intervals. Such a system is known as a 'fragmented' computer. An isolated computer in such a system must make access control decisions using the data it holds and the access request messages it receives. When there are large numbers of users (for example in a world-wide videotext service) it may be costly to store tables of all user identities and their public keys at all locations.

The system of operation in which the user's public key pk is included in the external capability avoids the need for local records of all users.

In order to establish a user's authenticity, the computer must decipher the enciphered combination so that the public key can be used to check the signature. If a symmetric cipher is used, the cipher key kos must be distributed to all parts of the system. If a public key cipher is used, those parts which do not need to create new capabilities need only be given the public key.

Any part of the system which holds the enciphered key may be allowed to create new capabilities, complying with the access rules of the system.

The programming and modification of a computer and a terminal forming part of the computer is not described in more detail than the above description since it is within the capabilities of those skilled in the art.

From the above it will be seen that the invention may take many other forms and be used in many other ways from those specifically mentioned. The computers whose capabilities are mentioned above have many different uses, for example in data bases and computer aided engineering.

CLAIMS

1. A method of granting access to a computer comprising
 - as a preliminary step,
 - storing a secret key in authentication apparatus together with enciphered information representing the capabilities to be granted by the computer and either the public key corresponding to the secret key or information which identifies the public key.
 - and as steps employed when access is to be granted,
 - using the authentication apparatus to form one part of an output message to contain the enciphered information and transforming as hereinbefore defined, using the secret key, a distinctive message to generate another part of the output message,
 - using the computer to decipher the enciphered information and inverse transform the said other part of the output message using the public key, and
 - comparing digital signals representing the result of the inverse transform with the digital signals representing the distinctive message or information derived therefrom and granting the required access only if the digital signals compared are the same.
2. A method according to Claim 1 wherein the said one part of the output message also includes the distinctive message.

3. A method according to Claim 1 wherein, when access is to be granted, the computer originates the distinctive message and supplies it to the authentication apparatus before the output message is formed.
4. A method according to Claim 1, 2 or 3 wherein the distinctive message is combined with the enciphered information and transformed with the enciphered information in generating the said other part of the output message. 5
5. A method according to Claim 4 including pre-processing the information for the said other part of the output message using a one-way function, and comparing the result of the inverse transform with a result obtained by pre-processing the distinctive message and the enciphered information in the same way before granting access. 10
6. A method according to any preceding claim wherein the distinctive message comprises at least one of the following: an indication of where the said output message stands in a sequence of such messages, the time of day, the date, and a random number.
7. A method according to any preceding claim wherein the authentication apparatus is a signature token or a workstation. 15
8. Authentication apparatus for providing access to a computer comprising
 - a store containing a secret key for carrying out a transformation as hereinbefore defined and enciphered information representing capabilities to be granted by a computer and either the public key corresponding to the secret key or information which identifies the public key,
 - input/output means for receiving and transmitting electrical digital messages to, and from, the apparatus, and
 - means for forming one part of an output message to contain the enciphered information and for transforming, using the secret key, a distinctive message, or a message determined therefrom, to generate another part of the output message.
 20
9. Authentication apparatus according to Claim 8 wherein the apparatus is arranged to form the said one part of the output message to contain the distinctive message. 25
10. Authentication apparatus according to Claim 8 or 9 wherein the apparatus is constructed to combine the distinctive message and the enciphered information before transforming the combination to form the said other part of the output message.
11. Authentication apparatus according to Claim 8, 9 or 10 arranged to pre-process the information from the said other part of the output message according to a one-way function in generating the said other part. 30
12. A computer programmed
 - to decipher one part of a message transmitted to the computer, the said one part containing, in enciphered form, information representing access to computer capabilities and a public key or information identifying the public key, and
 - to inverse transform another part of the message using the public key to determine whether the result after inverse transformation contains a predetermined distinctive message, and if so to provide the access conferred.
 35
13. A computer according to Claim 12 programmed to obtain the distinctive message from the said one part of the message for use in determining whether the said result contains the distinctive message. 40
14. A computer according to Claim 12 programmed to transmit the distinctive message to authentication apparatus when the apparatus initiates a request for access to capabilities of the computer. 45
15. A computer according to Claim 12, 13 or 14 for use where the said other part of the output message from the authentication apparatus is expected to include, in transformed form, the said one part of the message, wherein the computer is programmed to provide access to capabilities only if on inverse transforming the said other part of the output message, the public key and capabilities are as contained in the said one part. 50
16. A computer according to Claim 15 for use where the information for the said other part of the message is pre-processed according to a one-way function, wherein the computer is programmed to pre-process the said one part of the message according to a one-way function for use in determining whether the said other part of the message contains the said one part of the message. 55
17. Authentication apparatus which can easily be held in one hand and comprises
 - input/output means for receiving electrical digital messages to be "transformed" and for transmitting transformed messages,
 - an electrical store which is physically tamper-resistant holding a secret electrical digital key for use in carrying out transformation as hereinbefore defined, the key being so stored that it cannot be read out by applying signals to the apparatus,
 - transformation means for transforming, when enabled, an input message or a message related thereto using the secret key to generate an output message for transmission by the input/output means,
 - enabling means for enabling the transformation means on receipt of a personal input to the
 60

apparatus direct from a particular person or at least one of a particular group of persons, the personal input being specific to that person or those persons, and
a display for displaying at least part of the message to be transformed.

18. Authentication apparatus substantially as hereinbefore described with reference to Fig. 1
5 of the accompanying drawings. 5

19. An authentication method substantially as hereinbefore described with reference to Figs. 2 and 4 of the accompanying drawings.

20. A computer programmed substantially as hereinbefore described to co-operate with authentication apparatus in granting computer capabilities.